Warszawa, dn. 18.05.2022 r.

Rekordowa kara PUODO dla administratora – a kontrola podmiotu przetwarzającego

Czy korzystasz z usług podmiotów przetwarzających? Czy przykładasz szczególną wagę do odpowiedniej weryfikacji procesorów przed powierzeniem im danych osobowych do przetwarzania? A może zlecasz kontrolę prawidłowości przetwarzania danych w trakcie współpracy?

19 stycznia br. Prezes Urzędu Ochrony Danych Osobowych (dalej: PUODO) wydał decyzję w sprawie niewdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych. Z pełną treścią decyzji. można zapoznać się pod adresem: https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020

Sprawa dotyczyła naruszenia poufności danych oraz braku weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje przetwarzania zgodnie z wymogami RODO.

O współpracy z procesorem w praktyce pisaliśmy już wcześniej – np. tutaj: https://www.isecure.pl/blog/wspolpraca-z-procesorem-w-praktyce-kilka-waznych-kwestii/ . Niestety, praktyka pokazuje, iż administratorzy nie są świadomi, że w relacji z kontrahentami dochodzi w ogóle do powierzenia danych w rozumieniu przepisów o ochronie danych osobowych. A pamiętajmy, że RODO nakłada na podmioty po obu stronach liczne obowiązki, jak również prawa. Na bazie oceny powagi sytuacji, ale też wysokości nałożonych kar powstał niniejszy artykuł, w którym skupimy się wyłącznie na uprawnieniach administratora do inspekcji podmiotu przetwarzającego, czyli sprawdzenia czy dany podmiot spełnia właściwe środki mające zapewnić zgodność przetwarzania danych z wymogami RODO.

To właśnie po stronie administratora leży obowiązek uregulowania relacji z podmiotem przetwarzającym (procesorem). Odpowiedzialność bowiem za to spoczywa na samym administratorze.

Na co powinniśmy zwrócić szczególną uwagę?

Wybór administratora w zakresie współpracy z podmiotem przetwarzającym musi być zatem dobrze przemyślany i uważny. Administrator ma odpowiednie narzędzia, które pozwolą mu zweryfikować właściwy wybór wśród potencjalnych procesorów. Niewątpliwie, umowa powierzenia, która powinna być zawarta pomiędzy administratorem i procesorem i która wskazuje przedmiot uzgodnień pomiędzy stronami, będzie jednym z takich narzędzi. Stanowi bowiem gwarancję podmiotu przetwarzającego, w zakresie wdrożenia środków technicznych i organizacyjnych zapewniających zgodność przetwarzania danych z przepisami RODO, w szczególności w zakresie bezpieczeństwa przetwarzania.

Jednak, jak faktycznie dokonać weryfikacji podmiotu przetwarzającego? W tym zakresie bez wątpienia pomocne może być uprawnienia administratora określone w art. 28 ust. 3 lit. h RODO oraz art. 28 ust. 4 RODO. W treści tego artykułu, a dokładnie art. 28 ust. 3 lit. h RODO znajdziemy informację, iż administrator ma możliwość przeprowadzenia audytu u procesora – sprawdzającego poziom zgodności z wymaganiami RODO. Co więcej, warto również zauważyć i uzupełnić tę informację o fakt, iż podmiot przetwarzający ma obowiązek polegający na udostępnianiu administratorowi wszelkich danych niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO.
Popularne staje się również regulowanie w ramach umowy powierzenia uprawnienia po stronie administratora do przeprowadzenia audytu także u subprocesorów. Tendencja do uregulowania tego zagadnienia w ramach umowy wynika prawdopodobnie z treści art. 28 ust. 4 RODO. Zgodnie z nim podmiot przetwarzający może podpowierzyć dane osobowe jedynie na podstawie umowy zawartej ze swoim podwykonawcą, której treść zapewniać będzie stosowanie przez podwykonawcę środków gwarantujących przetwarzanie zgodnie z wymogami RODO. W interesie administratora pozostaje zatem zapewnienie sobie możliwości przeprowadzenia audytu u subprocesora, w celu utrzymania pełnej kontroli nad przetwarzanymi przez niego danymi osobowymi.

Krótko o prawie audytowania

Najczęściej zadawanym pytaniem przez administratora jest budzący wątpliwość zakres przeprowadzonego audytu. Podmiot przetwarzający udostępnia administratorowi informacje niezbędne do wykazania spełnienia obowiązków wynikających z przepisu art. 28 ust. 2, 3 i 4 RODO. Sprawdzenie może zatem dotyczyć następujących informacji:

- Czy podmiot przetwarzający korzysta z podwykonawców przetwarzających dane powierzone przez administratora na zasadach określonych pomiędzy stronami oraz zgodnie z art. 28 ust. 2 i 4? (w szczególności czy umowy podpisywane z podwykonawcami w sposób odpowiedni regulują kwestie związane z przetwarzaniem danych administratora)?
- Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, które umożliwiają procesorowi wsparcie administratora w odpowiadaniu na żądania osób, których dane dotyczą, w zakresie realizacji ich praw wynikających z RODO?
- Czy osoby biorące udział przy przetwarzaniu zostały zobowiązane do zachowania tajemnicy?
- Czy podmiot przetwarzający wdrożył mechanizmy/procedury, umożliwiające bezzwłoczne zgłoszenie naruszenia bezpieczeństwa danych osobowych?
- Czy dane nie są przekazywane przez podmiot przetwarzający do państw trzecich?

Mając na względzie obowiązek administratora wynikający z art. 28 ust. 1 RODO, nie bez znaczenia powinny również pozostawać następujące informacje:

- Czy podmiot przetwarzający stosuje fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych?

- Czy podmiot przetwarzający nadaje upoważnienia do przetwarzania danych osobowych?
- Czy podmiot przetwarzający prowadzi dokumentacje ochrony danych osobowych?
- Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania?
- Czy podmiot przetwarzający powołał inspektora ochrony danych?

Powyższe, wskazuje w jaki sposób i w jakim zakresie można dokonać sprawdzenia procesora. RODO jednak nie wskazuje wprost w jaki sposób administrator ma wykazać spełnienie tego wymogu.

Administrator powinien zatem podejmować takie działania, które pozwolą mu na uwierzytelnienie sprawdzenia procesora. Bowiem w przypadku kontroli ze strony organu nadzorczego, administrator musi wykazać, że dokonał dobrego wyboru podmiotu przetwarzającego, zapewniającego bezpieczeństwo danych osobowych. W tym wypadku, przywołanym dowodem może być raport z przeprowadzonych czynności audytowych czy kwestionariusz weryfikacyjny wypełniony przez procesora, dający gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających bezpieczeństwo przetwarzanych danych.

Administrator, w stosowanej formie sprawdzenia, powinien dokonać oceny poszczególnych środków zapewniających bezpieczeństwo przetwarzania danych według ustalonych kryteriów przyjętych np. w procedurze weryfikacji podmiotu przetwarzającego (tj. zgodność / częściowa zgodność / niezgodność).

Przepisy RODO, nie wskazują również terminu na przeprowadzenie weryfikacji podmiotu przetwarzającego. Wydaje się jednak niezbędnym, że sprawdzenie podmiotu przetwarzającego powinno nastąpić w pierwszej kolejności przed podpisaniem umowy powierzenia oraz faktycznym przekazaniem danych przez administratora. Ale to nie wszystko - weryfikacja podmiotu przetwarzającego powinna mieć miejsce również w trakcie trwania współpracy. Administrator powinien bowiem zawsze posiadać aktualne informacje na temat środków bezpieczeństwa wykorzystywanych przy przetwarzaniu danych osobowych, którego w jego imieniu dokonuje podmiot zewnętrzny. Tylko takie działanie należy uznać, za zapewniające spełnienie przez administratora obowiązku wynikającego z art. 28 ust. 1 RODO.

Podsumowując, administrator danych powinien przykładać szczególną wagę do odpowiedniej weryfikacji procesorów przed powierzeniem im danych osobowych do przetwarzania, a także bieżącego kontrolowania prawidłowości przetwarzania danych w trakcie współpracy. Pamiętajmy, że jeżeli administrator nie dysponuje wystraczającą wiedzą w zakresie RODO, zasobami kadrowymi oraz czasowymi może skorzystać z wyspecjalizowanych podmiotów zewnętrznych. Z art. 28 ust. 3 lit. h RODO wprost bowiem wynika, że podmiot przetwarzający ma umożliwić audyt administratorowi lub audytorowi upoważnionemu przez administratora. Brak jest zatem przeciwskazań, aby w tym zakresie,

administrator mógł skorzystać z podmiotów zewnętrznych specjalizujących się w prowadzeniu działań audytowych.

Olga Skotnicka – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.